FIXED FACILITY CHECKLIST (FFC) INSTRUCTIONS

Part II - Detailed Instructions

(DCID 6/9, Annex "A")

Revised: 2 August 2004

General:

HEADER/FOOTER:

DATE: Enter the date as applicable on all pages.

CLASSIFICATION: Ensure all pages are appropriately marked with the highest classification that appears on that page. Generally, all pages of the Fixed Facility Checklist will be classified Confidential at a minimum once it is filled in.

☑ *Preconstruction*: Check here if the SCIF has been constructed.
☑ *New Facility*: Check here if the SCIF has not been previously accredited.
☑ *Modified*: Check here if the SCIF is to be expanded, reduced, or changed.
☑ *Page Change*: Check here if you have administrative changes to make to the FFC. Ensure you place an asterisk (*) next to all changes.

Section A - General Information

1. SCIF Data:

   a. *Organization/Company Name*: Enter your organization or company name
   b. *SCIF Identification (ID) Number*: (If applicable) If it is an existing SCIF – this may not apply to new or preconstruction FFCs. DIA/DAC-2A will issue an ID number based on the sponsoring Agency or Military Department authorizing the establishment of the subject SCIF. *Issuance of this number does not constitute accreditation.*
   c. *Organization Subordinate to*: This identifies the organization in the security chain of command.
   d. *Contract Number & Expiration Date:* If a contractor facility, enter the contract number and expiration date for which this SCIF is being established for.
   e. *Concept Approval Date & By:* Enter the date of the Concept Approval/Validation document and the name of the validation organization/person that validated the SCIF requirement.
   f. *Cognizant Security Authority (CSA):* The Cognizant Security Authority, (CSA), as delegated by the SOIC, is responsible for implementing SCI security policies and procedures. SSO DIA/DAC-2A is the CSA for OSD, OJCS, DIA, DoD Agencies, DoD Field Activities, and Combatant Commands. (REF: DoD 5105.21-M-1, Chap. 1, para. 3)
   g. *Defense Special Security Communication System (DSSCS:)* (If applicable)

h. *DSSCS Message Address:* Include the message traffic address in which official correspondence shall be sent.
i. *DSSCS INFO Address:* Include any additional message traffic addresses in which official correspondence shall be sent as a courtesy. (If there are no DSSCS Message Addresses, please provide instructions, in the provided space on how you can receive official message traffic.)

2. SCIF Location:

   a. *Floor*: Enter the floor(s) the SCIF occupies. This is a key factor in determining some security measures that may be required.
   b. *Room Number(s)*: Enter the room number(s) of the entire SCIF area. Identify all room number(s) on all drawings submitted.

3. Mailing Address: Input if different from the SCIF Location.

4. E-Mail Address: Input the e-mail address of the facility (if applicable) or the primary responsible security officer.

5. Responsible Security Personnel:

   a. *DSN Telephone*: Input if available.
   b. *Home Telephone*: This field is optional. If inputted, it will only be used in emergencies for official use.
   c. *Secure Telephone:* Input the complete number of a dedicated secure telephone system, (i.e., red switch, NSTS, etc.).
   d. *Command or Regional Special Security Office:* (If applicable) Input the name of the command or regional Special Security Office here.
   e. *Command or Regional SSO Name:* Input the name of a point of contact at the Command or regional Special Security Office

6. Accreditation Data:

   a. *Category/Compartments of SCI Requested:* Enter the compartments of SCI that are to be worked within the SCIF.

   b. *Indicate the storage required:* Mark the appropriate block for the type of classified [SCI] storage you want accredited.
      1) OPEN Storage: SCI will not be stored within GSA-Approved safes. This storage type must be selected if the facility uses SCI computers that do not have removable hard drives.
      2) CLOSED Storage: All SCI is stored in GSA-Approved safes.
      3) Continuous Operations: SCIF will be used 24 hrs per day, 7 days per week. Unattended storage of SCI is not authorized.
      4) NONE: Select this type of storage if you are establishing a Secure Working Area or Temporary Secure Working Area.

c. *Indicate the Type of Facility:* Mark the appropriate block for the type of facility you want accredited.
    1) Permanent: Select this type of facility if this SCIF will be permanent. This is the typical selection.
    2) Secure Working Area (SWA): SCI will not be stored in this type of facility.
    3) Temporary Secure Working Area (TSWA): SCI will not be stored in this type of facility.
    4) Tactical: Select this type of facility if it will be Semi-Permanent

d. *Existing Accreditation Information*: Only applies to currently accredited SCIFs.
    1) Category/Compartments of SCI: Input the compartments of SCI that were previously authorized to be worked on within the SCIF.
    2) Accreditation granted by & on: Input the previous or current accreditation data, to include who issued the accreditation and when it went into effect.

7. Construction/Modification: Indicate whether or not all construction/modification has been completed? If construction is not complete, please indicate the estimated time of completion in the space provided.

    a. By indicating yes, it is presumed the facility is ready for accreditation or reaccredidation.

8. Inspections: List the organization who conducted the inspection as well as the date of the most recent security inspections or advice & assistance visits, (a.k.a. Security Assistance Visits, Staff Assistance Visits). *Attach a copy of the reports as applicable.*

9. Remarks: Enter any additional information (i.e., further explanation, co-utilization, etc.) which is pertinent to this section.

Section B – Peripheral Security

1. Describe building exterior security: Describe all security measures that are exterior to the building which houses the SCIF.

    a. Please indicate whether or not the building is located on a controlled compound or equivalent.

    b. Identify if there is a fence around the building. If so, please input the type, height and length. Also include all applicable information about fence alarms, lighting, building lighting, Cameras/Television (CCTV) and guards that are exterior to the building.

c. Exterior security measures may reduce or mitigate other recommended physical security construction and/or TEMPEST requirements.

2. Building: Describe the material used, thickness of building walls, type of windows, etc. in sufficient detail as to determine its benefit as a security barrier. Identify the method used to control building access during both duty & non-duty hours.

   a. Please ensure you provide a legible general building floor plan of SCIF perimeter on a 8.5" X 11" or 11" x 17" format.

3. Security In-Depth: Please identify/explain all external security attributes and/or features that the CSA should use to determine whether or not your facility has Security In-Depth.

   a. This information may be part of the above peripheral security attributes or may include other security layers not specified elsewhere in this section or the FFC.

Section C – SCIF Security

1. Access Control: Describe how access into and out of the SCIF is controlled during duty hours. List the manufacturer & model number of the access control devices used.

   a. Non-automated access control systems are mechanical or electro-mechanical access devices that do not have an automated means of tracking who and when a device was accessed.

   b. 128-bit encryption requirement for an automated access control system is only required when the device/equipment is located outside the SCIF and the line is accessible. Refer to DCID 6/9, Annex F for additional information on Personnel Access Control Systems.

2. Windows:

   a. *Acoustical Protection*: Usually only applies to accessible windows, (ground floor).
   b. *Secured against Opening*: If the windows are at ground level, are they locked or sealed? Are there any other forced entry protection features, (i.e., Bars, Grills, window film, etc.)?
   c. *Visual Protection*: Describe what measures prevent someone from seeing inside the SCIF, (i.e., blinds, drapes, opaque covering, etc.). Window film is usually not good enough because of the light reversal at night.

3. Ventilating Ducts which penetrate the SCIF Perimeter: Indicate all duct penetrations and their size on a separate floor plan or as an attachment. Please describe the type of protection installed if they are greater than 96 square inches, (i.e., 12"x 8").

4. Construction: Describe the material used, thickness of SCIF walls, floor, and ceiling in sufficient detail to determine its benefit as a security barrier.

Section D - Doors

1. SCIF Primary Entrance Door: Describe the materials used to construct the primary entrance door, its thickness, and any additional security features. Please indicate the primary entrance location on all floor plans.

2. SCIF Emergency Exit(s) & Other Perimeter Doors: Describe the materials used to construct the doors, their thickness, and any additional security features. Please indicate their locations on the floor plans.

3. Exterior Hinges: If door hinges are located outside the SCIF in an uncontrolled area, please identify how they are protected against removal.

4. Locking Devices: Describe the lock(s) used on the entrance and emergency exit doors. If a vault type door is used and it stands open during the day, please identify how the back of the lock is protected. *Be sure to identify the SCIF CSA and SCIF ID number of where the lock combinations are held.*

Section E – Intrusion Detection System (IDS)

1. General IDS Description:

   a. *IDS Company provider Name:* Input the name of the entire alarm system (if applicable) and/or the name of the company installing the system.

   b. *Interior Motion Detection Protection*:

      1) *Accessible Points of Entry / Perimeter or Storage Areas*: Please select one or the other.
      2) *Motion Detection Sensors*: List manufacturer and model number. Indicate their locations on the floor plans. If the sensors have removable covers, ensure they are equipped with tamper protection.

2. Are there any other intrusion detection equipment sensors / detectors in use? List manufacturer and model number of the contact sensor (Balanced Magnetic Switch (BMS)) on the door and any other sensors that may be in use.

a. Indicate their locations on the floor plans. If the sensors have removable covers, ensure they are equipped with tamper protection?

3. Does the IDS extend beyond the SCIF perimeter? This question refers to the capabilities located outside the SCIF perimeter, (i.e., at the monitoring station).

4. Do any intrusion detection equipment components have audio or video capabilities? This question refers to audio or video recording/monitoring capabilities that may exist in conjunction with motion sensors or like equipment.

5. External Transmission Line Security IDS: Identify the type of transmission line security. Is it 128-Bit encryption or greater? If not please identify the type of alternate line security you propose. Be sure to list the manufacturer and model of the line supervision as well as if it has any wireless capabilities. *For more information on encryption standards check out this website: http://csrc.nist.gov/cryptval/des.htm*

6. IDS Emergency Power: Identify the type/duration of emergency back-up power.

7. Vent & Ductwork Protection: If applicable, list manufacturer & model number of vent/duct sensors.

8. IDE Location: Indicate the location of all Intrusion Detection Equipment (IDE) (i.e., including the Premise Control Unit (PCU)) on the SCIFs floor plan. Identify the manufacturer & model number of the PCU.

9. IDS Annunciation Panel Location: Identify the room number, building & address of the monitoring station. Please indicate whether it is within the same controlled compound or building.

10. IDS Response Personnel: Identify who is responsible for responding to alarms which occur within the SCIF. Indicate their clearance level. *Response times may not be available for a Preconstruction FFC.*

a. Ensure a written support agreement has been established for monitoring and/or responding to alarms. These agreements shall identify the response time of the response force and SCIF personnel, responsibilities of the response force upon arrival, maintenance of SCIF points of contact and length of time response personnel are required to remain on-site.

11. IDS Testing: Is the IDS tested every 6 months and are the records maintained? *Testing information may not be available for a Preconstruction FFC.*

12. Remarks: Enter any additional information which is pertinent to the security of SCIF IDS.

Section F – Telecommunication Systems and Equipment Baseline

1. Method of On-Hook Audio Protection: Choose ONE option.

    1) *Telephone Security Group (TSG)-6 Approved Telephones*: List manufacturer, model number and TSG approval number. If this option is chosen, no other on-hook audio protection is required.
    2) *TSG-6 Approved Disconnect Devices*: List manufacturer, model number and TSG approval number. If this option is chosen, no other on-hook audio protection is required.
    3) *Computerized Telephone System (CTS)*: If yes, answer questions 3.a-3.i on the FFC. If this option is chosen, no other on-hook protection is required.

2. Do all unclassified telephones within the facility have a hold, mute and/or push-to-talk [handset] capability, (for off-hook audio protection)? Answer yes to verify that all unclassified telephone do have adequate off-hook audio protection. If no, please explain what measures are used to protect the telephone when the user leaves the telephone temporarily off-hook and unattended.

3. Automatic Telephone Call Answering: List manufacturer and model number of any answering machines or voice mail systems used. Identify their location on the facility floor plan.

4. Are any Multi-Function Office Machines (M-FOMs) used within the SCIF? M-FOMs are electronic equipment that can be used as network or standalone printers, facsimile, and copiers?

5. Are there any Video Teleconference (VTC) Systems installed? Ensure you identify the classification of the VTC system and its location within the SCIF.

6. Does the SCIF have any automated environmental infrastructure systems? These are unclassified computer controlled systems that are connected to the public switch telephone network or like connection with the capability to connect to from a remote location for monitoring, access, and external control/modification to features or services.

Section G – Acoustical Protection

1. Do all areas of the SCIF meet acoustical protection requirements of Annex E? Answering YES to this question validates that all SCIF perimeter walls meet a Sound Transmission Class (STC) of 45 or better, (Sound Group 3). *May not be available for a Preconstruction FFC.*

2. Are there any amplified audio systems used for classified information? These typically Video Tele-Conferencing (VTC) systems or Public Address (PA) system used in an auditorium, etc.

    a. Answering YES will require you to answer a follow-up question: *Are the walls/ceilings/floor of the room where the amplified audio system resides acoustically treated to meet a STC of 50 or better?*

3. Is the SCIF equipped with a public address, emergency / fire announcement or music system originating outside the SCIF? Please select YES to this question if the SCIF has any PA, emergency notification, or music system that is installed within the SCIF and has external components or signal lines that egress the SCIF perimeter.

    a. It may be helpful to provide a drawing, with the manufacturer, make, model and its operating function/configuration and its location on larger building map.

    b. Please explain how those systems are protected. (These systems may require additional TEMPEST/Technical Security Countermeasures.)

Section H – Classified Destruction Methods

1. Destruction Methods: Identify the method used for destruction of sensitive/classified waste. If a commercial destruction device is used, list manufacturer and model number. If specialized destruction methods are used for any material, describe them fully.

2. Remarks: Enter any additional information which is pertinent to the destruction methods for SCIF security. Also use this area if more than one type of device is used. Be sure to list all manufacturer and model numbers for all devices.

Section I – TEMPEST/Technical Security

1. Does the facility electronically process classified information? Please identify if the SCIF uses classified computer systems and at what level they operate at. If YES, please ensure you submit an initial or updated TEMPEST Addendum to the Fixed Facility Checklist, (DoD 5105.21-M-1, Appendix J).

2. Has the CSA's *Certified TEMPEST Technical Authority* (CTTA) required any TEMPEST countermeasures? If the CSA's CTTA has conducted a countermeasures review, please identify all recommended or required countermeasures and annotate all countermeasures that were installed.